# Security in IoT Systems using Physical Unclonable Functions

**Vedavyas Paritala[1], Manjula M[2]**

*[1]Student, Department Computer Science and Engineering, Atria Institute of Technology, Bangalore, India*
*[2]Assistant Professor, Department Computer Science and Engineering, Atria Institute of Technology, Bangalore, India*

---------------------------------------------------------------------***---------------------------------------------------------------------

**Abstract –** *In the past, just mobiles and PCs were associated with the web yet in the new time with the coming of new innovations different things like surveillance cameras, microwaves, vehicles and modern hardware's are presently associated with web. This system of things is known as the web of things. There are now 6 billion gadgets on the web and inside a couple of years these number is foreseen to scale to 20 billion gadgets. As of late, a huge number of surveillance cameras were penetrated to dispatch a DDOS assault that caused Twitter blackout. IoT arrangements isn't simply programming however a whole environment of equipment, programming, cloud, web and versatile interfaces. This environment isn't exceptionally full grown and there are as yet significant concerns sneaking around IoT reception fundamentally because of security dangers. To address this issue, we present light-weight shared verification conventions for IoT frameworks dependent on Physical Unclonable Functions (PUFs).A security and execution examination of the conventions shows that they are hearty against various kinds of assaults, but on the other hand are very efficient as far as calculation, memory, vitality, and correspondence overhead .*

***Key Words*: DDOS, Penetrated, Physical Unclonable Function, Framework, Security, Versatile interfaces.**

## 1. INTRODUCTION

The quantity of IoT gadgets has been expanding quickly over the previous decade, dwarfing people by a proportion 2 to 1 starting at 2019. There are as of now 6 billion gadgets on the web and inside a couple of years these number is foreseen to scale to 20 billion gadgets.

IoT is imagined as the empowering innovation for urban areas, power frameworks, human services, and control frameworks for basic portions and open foundation.

This decent variety, expanded control and collaboration of gadgets, and the way that IoT frameworks utilize open systems to move a lot of information make them an ideal objective for digital assaults.

IoT security and human wellbeing are attached to one another, e.g., causing mishaps by upsetting vehicular systems, putting a patient in danger by messing with a body arrange, causing power outages by meddling the brilliant matrix, and causing mishaps in atomic reactors and so on

## 2. REVIEW OF LITERATURE

1. Hyun-Jin Kim, Hyun-Soo Chang, Jeong-Jun Suh, A Study on Device Security in IoT Convergence, 2016 IEEE, in this paper I learnt various sorts of IoT gadgets and dangers of every classification and diverse security necessities of IoT devices.[1]
2. Debdeep Mukhopadhyay, PUFs as Promising Tools for Security in Internet of Things, 2015 IEEE, in this paper I have examined the utilization of Physically Unclonable Functions (PUFs), as an equipment security crude for authentication.[4]
3. Shaza Zeitouni, Yossef Oren, Christian Wachsmann, Patrick Koeberl, and AhmadReza Sadeghi, Remanence Decay Side Channel: The PUF Case, JUNE 2016 IEEE, in this paper I have considered a side-channel assault dependent on remanence rot in unpredictable memory and how it very well may be misused viably to dispatch a non-intrusive cloning assault against SRAM physically unclonable functions (PUFs).[3]
4. Albandari Alsumayt, John Haggerty, Ahmad Lot, Detect DoS assault utilizing MrDR technique in blending two MANETs 2016 IEEE, in this paper I have concentrated how to assault during the time spent combining two MANETs.
5. AkashdeepBharadwaj, Dr.GVB Subramanyam, Dr.Vinay Aasthi, Dr.Hanumat Sastry, Solutions for DDos assaults on cloud 2016 IEEE. A multi-layered Network Architecture forDDos relief has been proposed wherein mixture cloud model is used.[5]
6. Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito, Mark Vinkovits Denial-of-Service discovery in 6LoWPAN based Internet of Things, 2013 IEEE, in this paper a disavowal of administration (DOS) identification design for 6LoWPAN (ivp6 over low force remote work force territory organize) is proposed.[2]

## 3. SYSTEM ARCHITECTUR

The IoT arrangements today, have been conveyed with the emphasis on speedy time to showcase tending to significant client necessities to have an edge against different contenders. There is practically no venture on planning these arrangements thinking about security angles. Most IoT arrangements today have gadgets sending information to cloud that have no personality checks accordingly permitting assailants to fabricate programming clones and transfer terrible information in a similar organization to IoT backend in cloud. Plus, gadgets send information in clear content over web to cloud making these solutions vulnerable for attacks.

Problem 1. Identification of authentic devices to prevent malicious clones to be registered with the system and upload malicious data.

Before introducing the proposed convention, we first present a short prologue to PUFs in this segment. A PUF might be viewed as an exceptional physical component of a gadget, much the same as the biometric highlights of people, for example, fingerprints. A decent definition of a PUF is given in as "a statement of an inalienable and unclonable occurrence specific highlight of a physical article". The most striking property of a PUF is that it can't be duplicated utilizing cryptographic natives, rather, it requires a physical premise. In addition, the expression "physically unclonable" implies that it very well may be appeared through physical thinking that it is incredibly hard or even difficult to deliver a physical clone of a PUF. So, the thought behind utilizing a PUF in IoT frameworks is that simply like individuals, each gadget will have an exceptional fingerprint as a PUF and this fingerprint can't be recreated or cloned. In somewhere else, a PUF is defined as "A Physical Unclonable Function (PUF) is a function that maps a lot of difficulties to a lot of reactions dependent on an obstinately mind-boggling physical framework".

In this way, a PUF can be considered as a function, which takes a test as a series of bits and produces a reaction as a series of bits. We speak to a PUF as a function P as follows:

$$\mathbf{R = P(C)}$$

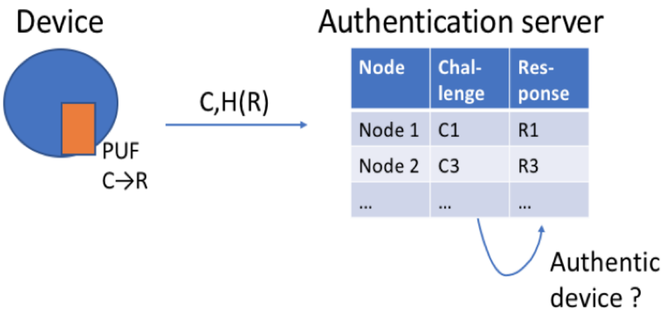
where R is the response of a PUF, while C is the challenge given to the PUF. A challenge C and its response R from a PUF is called a challenge response pair (CRP). PUFs have the following properties in terms of the response:

1. The PUF produces the same response with the same challenge with high probability even if the same challenge is used multiple times.

**Table -1:** Notations

| Notation | Description |
|---|---|
| $ID_i$ | ID of the IoT devices |
| H(X) | Hash of X |
| $\|\|$ | Concatenation operator |
| $\{M\}_k$ | Message M is encrypted using key K |
| $C^i$ | Challenge for the i-th iteration |
| $R^i$ | Response of the respective PUF for $C^i$ |

2. The same challenge will produce responses far apart with high probability if it is input to different PUFs.



| Node | Chal-lenge | Res-ponse |
|---|---|---|
| Node 1 | C1 | R1 |
| Node 2 | C3 | R3 |
| ... | ... | ... |

**Fig -1: PUF Authentication**

## 4. PROPOSED PUF BASED MUTUAL AUTHENTICATION AND KEY EXCHANGE PROTOCOL

In this segment we present the proposed mutual authentication protocol. The accompanying situations are considered for common verification: An IoT devices needs to set up an association with a server in the data center.

1. Protocol: IoT Device and Server Mutual Authentication The proposed mutual authentication protocol for the situation when an IoT devices and a server need to speak with one another is appeared in Figure. The means are as per the following: IoT gadget IDA sends its ID, IDA, and a Randomly created nonce, N1, to the server.
2. The server attempts to find IDA in its memory and if the pursuit bombs the confirmation demand is dismissed. Something else, the server peruses the CRP (Ci, Ri) put away in its memory for this gadget. The server at that point creates an irregular number RS1 and utilizations Ri to shape the encoded message MA = {IDA, N1, RS1} Ri. The server at that point sends Ci, MA, and the message verification code (MAC) to the IoT gadget IDA in message 2 in Figure 2. The MAC guarantees information uprightness and newness. The first two parameters in the MAC work guarantee information respectability while the last parameter, i.e., RS1 fills in as the newness identifier for the source, which for this situation is the server. A similar methodology is followed for information uprightness, message newness, and source identifier all through the convention.
3. IOT Devices IDA produces Ri utilizing its PUF and challenge Ci as surrendered (1). The gadget at that point gets RS1 utilizing Ri and verifies the source, respectability, and newness of the message utilizing the MAC. In the event that verification falls flat, IoT gadget IDA ends the confirmation. Else, it produces an arbitrary number NA and registers the new reaction Ri+1 by utilizing the new test H (NA k RS1) and its PUF. This new CRP (Ci+1, Ri+1) will be utilized for future validations. IoT gadget IDA at that

point sends an encoded message MS = {IDA, RS1, NA, Ri+1} Ri and the relating MAC to the server and afterward erases all the impermanent factors put away in its memory including RS1, NA, Ri, Ci+1, and Ri+1.

4. The server figures NA and Ri+1 utilizing Ri and verifies the MAC. On the off chance that the verification comes up short, the server dismisses the validation. Something else, shared confirmation is viewed as complete and the two substances would now be able to shape a meeting. We can utilize RS1 and NA to develop a meeting key as follows H(RS1) ⊕H(NA). (2) We note that the meeting key is developed utilizing the hash of the two arbitrary nonce RS1 and NA. In this manner, regardless of whether the meeting key is gotten by an enemy, he/she despite everything can't figure Ri.

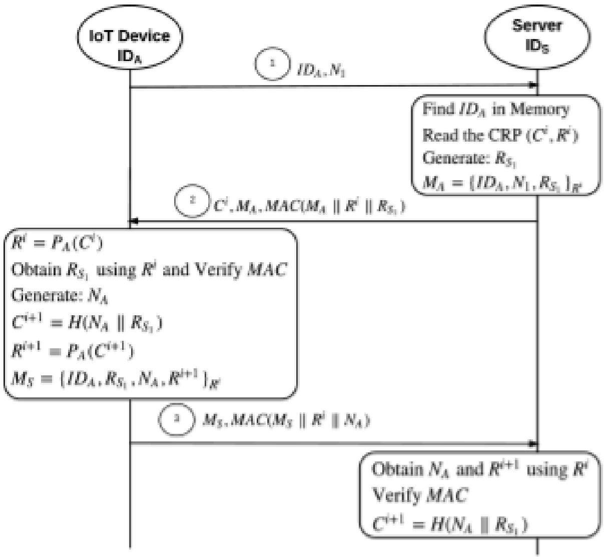
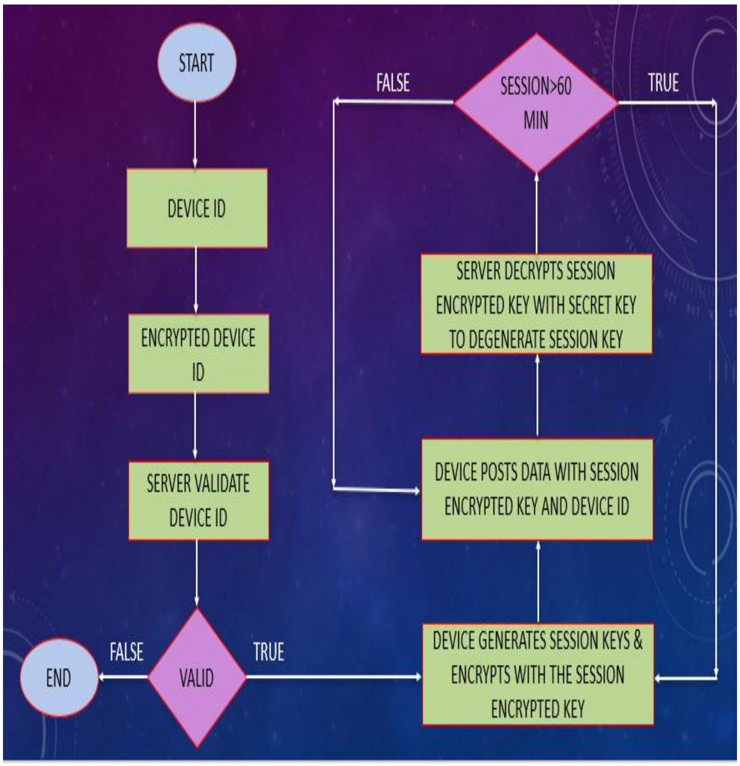

IoT Device $ID_A$
Server $ID_S$
1 $ID_A, N_1$
Find $ID_A$ in Memory
Read the CRP $(C^i, R^i)$
Generate: $R_{S_1}$
$M_A = \{ID_A, N_1, R_{S_1}\}_{R^i}$
2 $C^i, M_A, MAC(M_A \| R^i \| R_{S_1})$
$R^i = P_A(C^i)$
Obtain $R_{S_1}$ using $R^i$ and Verify $MAC$
Generate: $N_A$
$C^{i+1} = H(N_A \| R_{S_1})$
$R^{i+1} = P_A(C^{i+1})$
$M_S = \{ID_A, R_{S_1}, N_A, R^{i+1}\}_{R^i}$
3 $M_S, MAC(M_S \| R^i \| N_A)$
Obtain $N_A$ and $R^{i+1}$ using $R^i$
Verify $MAC$
$C^{i+1} = H(N_A \| R_{S_1})$

**Fig -2:** Mutual Authentication for IoT device and server

## 5. FLOWCHART

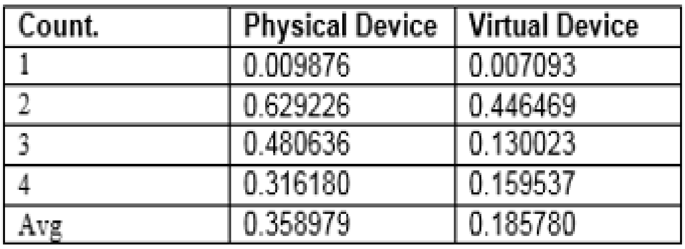
Device before uploading data to cloud, executes authentication module which prevents clones from being authenticated. The authentication module is described below and also illustrated in the flowchart


START
DEVICE ID
ENCRYPTED DEVICE ID
SERVER VALIDATE DEVICE ID
VALID
FALSE
END
TRUE
DEVICE GENERATES SESSION KEYS & ENCRYPTS WITH THE SESSION ENCRYPTED KEY
DEVICE POSTS DATA WITH SESSION ENCRYPTED KEY AND DEVICE ID
SERVER DECRYPTS SESSION ENCRYPTED KEY WITH SECRET KEY TO DEGENERATE SESSION KEY
SESSION>60 MIN
FALSE
TRUE

**Flowchart**

## 6. RESULTS

The authentication, encryption and detection of clones happens within seconds. The authentication starts and end times were recorded in logs and the averages across physical and virtual devices is reported in table below. As one can see from Table, the average timings are not growing exponentially as count of devices are increasing.



| Count. | Physical Device | Virtual Device |
|---|---|---|
| 1 | 0.009876 | 0.007093 |
| 2 | 0.629226 | 0.446469 |
| 3 | 0.480636 | 0.130023 |
| 4 | 0.316180 | 0.159537 |
| Avg | 0.358979 | 0.185780 |

**Fig -3:** Authentication time taken in seconds

## 7. CONCLUSION

This paper introduced common verification conventions for two unique situations in IoT frameworks: (I) for situations when an IoT gadget and a server need to speak with one another, and (ii) for the situation when two IoT gadgets need to speak with one another. The proposed conventions depend on a test reaction component utilizing PUFs and have the one of a kind securities highlights of not sparing any insider facts in the IoT gadgets, while keeping the capacity prerequisites at the server to the base. In addition, a meeting key can likewise be established using the proposed protocols. Performance analysis of the proposed conventions shows that they have low calculation, stockpiling, and correspondence overhead. Be that as it may, to utilize these conventions for applications with severe planning prerequisites, for example, vehicular systems, it is attractive to additionally diminish the idleness of verification by decreasing the quantity of messages traded between the substances.

## ACKNOWLEDGMENT

I acknowledge those who have supported me to do things in a better way and it would include my guide Prof. Manjula m for providing the right path throughout this research and giving in her encouragement and support. We are thankful to the authorities of Atria Institution of Technology, Bangalore for all the support and guidance.

## REFERENCES

[1] Hyun-Jin Kim, Hyun-Soo Chang, Jeong-Jun Suh, A Study on Device Security in IoT Convergence, 2016 IEEE.

[2] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito, Mark Vinkovits Denial-of-Service detection in 6LoWPAN based Internet of Things, 2013 IEEE.

[3] Shaza Zeitouni,Yossef Oren,Christian Wachsmann, Remanence Decay SideChannel: The PUF Case, 2016 IEEE.

[4] Debdeep Mukhopadhyay, PUFs as Promising Tools for Security in Internet of Things, 2015 IEEE.

[5] Akashdeep Bharadwaj,Dr. GVB Subramanyam, Dr.Vinay Aasthi,Dr.Hanumat Sastry,Solutions for DDos attacks on cloud, 2016 IEEE.

[6] Detect DoS attack using MrDR method in merging two MANETs, Albandari Alsumayt , John Haggerty , Ahmad Lot, IEEE 2016